

UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Regional

National

International

Banking and Finance Industry

**Chemical and Hazardous
Materials Sector**

Commercial Facilities

Communications Sector

Critical Manufacturing

Defense Industrial Base Sector

Emergency Services

Energy

Food and Agriculture

**Government Sector (including
Schools and Universities)**

**Information Technology and
Telecommunications**

National Monuments and Icons

Postal and Shipping

Public Health

Transportation

Water and Dams

**North Dakota Homeland Security
Contacts**

UNCLASSIFIED

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

(Minnesota) State to ask 3M to pay for environmental damage. The State of Minnesota will ask 3M to pay for environmental damage due to contamination from the company's operations in Cottage Grove. 3M manufactured chemicals known as PFCs, used in stain and fire-resistant materials, until 2002. The chemicals seeped from disposal sites into the Mississippi River. The state imposed fish-consumption advisories on the river as a result of the contamination. 3M has paid for cleanup, and for improvements to public and private water systems. But now, according to the Minnesota Pollution Control Agency, the company will be asked to pay for damage to the state's natural resources. Source: <http://minnesota.publicradio.org/display/web/2010/06/24/3m-pfc-pollution/>

(Minnesota) Woodlands National Bank targeted in 'phishing' scam. Woodlands National Bank, with a branch office in Cloquet, Minnesota, has been taking a lot of heat lately — through no fault of its own. The bank has been the brunt of an elaborate e-mail, phone and text message fraud that has provoked literally hundreds of phone calls weekly, according to a local branch manager. The Woodlands National Bank name and logo have been used without the company's consent or knowledge in "phishing" schemes aimed at acquiring sensitive information from unsuspecting consumers. The branch manager said that the perpetrators used a variety of methods to randomly contact people residing in the customer area of the bank's various branch offices. In most cases, the message informs the recipient that their account has been temporarily suspended, and requests proprietary information in order to bring it back on line. In the most recent telephone scam, a recorded message asks for recipients to input their debit card numbers in order to reactivate their accounts. She added that Woodlands National Bank does not send any sort of "alert messages" via e-mail, phone or text messages and never initiates a request for sensitive information through those means. Source: <http://www.pinejournal.com/event/article/id/20640/group/News/>

(Minnesota) Havoc on Albert Lea area farms after storms. A pair of storms swept tornadoes for more than 20 miles June 17 in southern Minnesota. The severe weather knocked out power and devastated a handful of farms near Albert Lea. For some, their livelihoods were all but wiped out. The storm blew down a farmer's 3,200-head hog farm. County officials said 15 people were injured, one of them fatally, as twisters skipped across the open farmland between Albert Lea and Blue Earth. The Freeborn County administrator said the first count of damaged buildings put the number over 60, and many of them were total losses. "If you know Freeborn County at all, it went through the rural areas of the county, therefore farms and small acreage homesteads, barns, sheds, those types of structures were in the way of the tornado, as were several hog confinement operations," he said. "So we have animal issues out there. Several feed lots, so that compounds it." Officials in the area said it may be

UNCLASSIFIED

UNCLASSIFIED

days before they get power restored and roads cleared. Source:

<http://minnesota.publicradio.org/display/web/2010/06/18/albert-lea-tornado-severe-weather/>

(Montana) Montana tornado rips roof off sports arena. A tornado ripped through two Billings, Montana neighborhoods, peeling the roof off a sports arena and several buildings. No deaths or major injuries were reported. The tornado touched down at about 4:30 p.m. June 20, running through Main Street and damaging about 10 small businesses in the city's northeast area before quickly hopscotching toward the 10,000-seat Rimrock Auto Arena about a half-mile away. Wind speeds from the tornado were estimated to range between 111 and 135 mph. The only reported injury was from someone hit in the head by a hailstone. City officials were also dealing with power outages and flooding from the storm, which sent about 2 feet of water into many streets. Source: <http://www.google.com/hostednews/ap/article/ALeqM5hHcrgfHj7ce14kUZTYsvqUIXfnQD9GFNSPG1>

(Montana) Pine Beetles force measures in recreation areas. Beaverhead-Deerlodge National Forest officials in southwest Montana said they will be applying insecticides at recreation sites throughout the forest during the next few weeks. The U.S. Forest Service (USFS) said the insecticide is needed because of the current mountain pine beetle epidemic that is destroying vast numbers of trees across the forest, including trees in recreation areas and campgrounds. "Campground users will notice packets stapled to trees. These 2"x2" packets are Verbenone and/or MCH and are used to ward away bark beetles in areas that we cannot spray the Carbaryl pesticides because of being too close to water," said the USFS reforestation forester. Source: <http://www.kxlf.com/news/pine-beetles-force-measures-in-recreation-areas/>

(Montana) Evacuated families on reservation not back home yet. Approximately 35 people voluntarily evacuated their homes on the Rocky Boy's Indian Reservation in Montana on Saturday after a problem arose at a dam there. The new evacuees were in addition to the 22 families evacuated Friday afternoon, who have yet to return to their homes. "We are in a Level 2 situation with our upper agency dam," the incident commander for the Chippewa Cree Tribe's disaster emergency services said late Saturday night. A Level 2 incident means "there is a problem arising [with the dam], not imminent danger," he said. He noted that though there was a problem, the dam had not cracked. He also said the situation had been stabilized as of 10:45 p.m. Saturday. The voluntary evacuations came after 22 families were evacuated Friday as a precaution and because some nearby roads washed out. All drainages throughout the reservation were experiencing flooding, the tribe said in a statement Friday. The Jon Morsette Vo-Tech Center was made available for residents displaced because of the high water. The American Red Cross of Montana provided 36 cots and other services at the center. Over the last four days, Rocky Boy received 4.8 inches of precipitation, according to the National Weather Service in Great Falls. Source: <http://www.greatfallsribune.com/article/20100620/NEWS01/6200319>

(South Dakota) New dam being built in Skunk Creek to prevent future flooding. As flooding still plagues parts of South Dakota, Sioux Falls Public Works is accelerating plans to raise levees along the Big Sioux River and put a dam in place to help protect against future flooding. Getting these structures up now is something that public works said benefits the city. Levees will be raised on Skunk Creek and on the Big Sioux River near 41st Street with a dam helping control water flow. The future dam is not intended to create energy but to act as a security gate for diverted waters should there be too much flooding on the Big Sioux River for the spillway on the north side of town to handle. "Here

UNCLASSIFIED

UNCLASSIFIED

we have a chance of hitting a flood every year,” said the principal engineer, “there’s not that much of a chance but there is a chance each year that you could have back to back 1 percent flooding.” In the event of a massive flood, the spillway can only release a certain amount of water, so the dam would then close to prevent flood water from Skunk Creek from flowing into the diverted spillway water and causing major flooding for the homes and businesses from 41st Street to Russell Street. Public works said that without help from city leaders the project would take years to finish. Source:

<http://www.ksfy.com/Global/story.asp?S=12673839>

(South Dakota) Brake failure led to chemical spill near Mitchell. Authorities said brake failure led to a weekend truck accident northeast of Mitchell, South Dakota in which farm chemicals were spilled near the James River. A Davison County sheriff’s deputy said a 34-year-old man was headed downhill when his brakes went. He suffered minor injuries in the rollover crash Saturday night. He was not cited. About 25 gallons of herbicide and 350 pounds of dry fertilizer spilled. The state Department of Environment and Natural Resources said the driver will be responsible for cleanup costs. Authorities said the accident could have been worse because the man’s truck narrowly missed a natural gas valve installation. Source: <http://www.ktiv.com/Global/story.asp?S=12682959>

NATIONAL

(Texas) FAA approves Predator drone to monitor Texas border. The Federal Aviation Administration (FAA) June 23 approved an unmanned aircraft to monitor 1,200 miles of the border, from El Paso to Brownsville, according to a Texas representative. “Today marks a critical next step in securing the Texas-Mexico border. By permanently positioning this aircraft in Texas, [Customs and Border Protection] (CBP) can further combat illegal activity along our southern border,” the representative said in a statement. “For five years, other southern border states have benefited from this technology and this will ensure Texas has the same tools in the box to combat the spectrum of threats we face.” The representative’s press release said the plane will be based in Corpus Christi. Earlier this month, CBP began flying a remotely piloted aircraft based in Arizona over a portion of West Texas. FAA’s most recent approval will allow CBP to fly over the remainder of the Texas-Mexico border along the Rio Grande. In addition, CBP will patrol the state’s coastline along the Gulf of Mexico. Known as a Predator B, the aircraft can fly for up to 20 hours and provide to CBP real-time, critical-intelligence information from attached cameras, sensors and radar systems. Source:

<http://aviationblog.dallasnews.com/archives/2010/06/faa-approves-predator-drone-to.html>

Storms pelt Midwest, cause flooding in Indiana. Central Indiana residents fled flooded neighborhoods Tuesday, including in Avon west of Indianapolis after two days of strong thunderstorms caused a retention lake to overflow an earthen dam threatening 32 homes and 16 trailers. Residents in other parts of Indiana and Midwestern states had to deal with flooding and tornadoes brought on by several days of storms. The storms that pelted the Midwest weakened as they moved east Tuesday, but the National Weather Service said another wave was moving into Iowa, Illinois, and Indiana. In Edna Mills, about 10 miles east of Lafayette, Ind., officials called for a voluntary evacuation as a small creek rushed over its banks, surrounding about three dozen homes and covering roads. School buses and boats were brought in to help residents who wanted to leave. Further south, water from a retention lake overflowed the Indian Head Lake Dam and forced crews to evacuate nearly 50 residences. Witnesses in central Illinois reported tornadoes near the Indiana border, while flash floods covered roads in Pana, Fulton and Vermilion County. Tornadoes were

UNCLASSIFIED

UNCLASSIFIED

spotted near Hoopston and Rossville, and the American Red Cross said 26 families were forced out of their apartments after strong winds blew the roofs off several buildings in Beardstown. The Indianapolis Department of Public Works was offering sandbags to residents. Source: <http://www.google.com/hostednews/ap/article/ALeqM5hP4Ms7EkAI5UtMVI3-49mTCPaKmQD9GGIABOO>

Internal BP document claims Gulf oil gusher jetting up to 100,000 barrels per day. U.S. outrage mounted against BP as the oil spill reached its two-month mark and an internal BP document showed as many as 100,000 barrels of oil could be gushing daily into the Gulf of Mexico. The document showed the energy giant's own worst-case scenario of the amount of leaking oil at possibly 20 times more than its early public estimates. The latest round of recriminations came after a week of White House arm-twisting prodded BP to agree to a \$20-billion fund to pay claims, and a stepped-up oil recovery effort in the Gulf. Media reports of BP's CEO attending a yacht race off the Isle of Wight, the day after he stepped down from managing the oil leak on a daily basis, set off one of the sharpest expressions yet of administration anger with BP. Over the past week, the British energy giant has called in more ships and equipment to the area, announced it was ahead of schedule in drilling the relief wells — seen as the best chance at killing the leak — and said it would significantly boost the amount of oil captured from its busted well. But a key U.S. Congressman, a vocal critic of BP and its handling of the disaster, lashed out at the firm after releasing an internal BP document that showed the energy giant's own worst-case, saying the firm was “either lying or grossly incompetent.” Source: <http://rawstory.com/rs/2010/0621/internal-bp-document-claims-gulf-oil-gusher-jetting-100000-barrels-day/>

INTERNATIONAL

Fake ATM dupes China bank customers. Thieves in Beijing set up a fake ATM machine that recorded the bank details of unsuspecting users whose accounts were later robbed, in the first such scam discovered in China, state press said June 23. Having duped bank customers into revealing their account details, the thieves forged duplicate bank cards to drain their accounts, China Central Television said. The machine was bought from a legitimate manufacturer, but was not affiliated to any bank, it added. The ATM was placed on a busy corner in central Beijing and advertised that it could accept many major credit and bank cards, but all transactions resulted in an error message, the official China Daily reported. According to the paper, one man who used the machine was robbed of 5,000 yuan (\$735), while another person had his bank account “drained” of an unspecified amount. No arrests have yet been made. Source: <http://www.google.com/hostednews/afp/article/ALeqM5jG4j6DtXkofKOOcLmUAsOO0tcWgg>

Al Qaeda front says it bombed Iraq bank; 18 die. An al Qaeda front group claimed responsibility June 23 for bombing a state-run investment bank, gloating over its ease in penetrating security in an attack that killed at least 18 people. The June 20 attack on the Trade Bank of Iraq was meant to expose the weakness of the country's stalled government, according to a statement posted on the Web site of the Islamic State of Iraq. The statement called the bank a “stronghold of evil” because it was established to attract foreign investment. The group, which is allied with al Qaeda, taunted the government for its inability to keep the peace. The same group claimed responsibility for the recent strike on the Central Bank of Iraq, the nation's treasury, in which at least 26 died in a commando-style

UNCLASSIFIED

UNCLASSIFIED

assault by bombers and shooters. Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/06/23/MNKC1E3VET.DTL>

Rains burst levee in southern China, 88,000 flee. Torrential rains burst a dike in southern China, sending 88,000 people fleeing their homes and prompting China's top leaders to call Tuesday for stepped-up rescue operations. Floodwaters breached the Changkai levee on the Fu River in Jiangxi province late Monday, forcing residents to relocate from their homes in the nearby city of Fuzhou, the official Xinhua News Agency reported. No casualties have been reported. Storms have pounded southern China for more than a week, killing at least 199 people, with 123 still missing, as landslides have cut off transportation, and rivers and reservoirs have overflowed. In some places, floodwaters reached nearly to the second story of buildings, while in others only the tops of trees were visible. Soldiers unloaded stacks of rowboats as they raced to rescue stranded residents. The China Central Television report said some 88,000 people have been displaced. Army and volunteer rescue teams have been working around the clock near Fuzhou to sandbag vulnerable areas. Flooding has affected more than 10 million residents across southern China, with heavy storms expected to move south in the coming days toward Fujian and Guangzhou provinces. China sustains major flooding annually along the mighty Yangtze and other major rivers, but this year's floods have been especially heavy, spreading across nine provinces and regions in the south and along the eastern coast. Source: http://news.yahoo.com/s/ap/20100622/ap_on_re_as/as_china_flooding;_ylt=AgXTjhCA7OrcUqmJ62eWuPIBxg8F;_ylu=X3oDMTJudGtmZmg3BGFzc2V0A2FwLzlwMTAwNjlyL2FzX2NoaW5hX2Zsb29kaW5nBHBvcwMzBHNIYwN5bl9wYWdpbmF0ZV9zdW1tYXJ5X2xpc3QEc2xrA3JhaW5zYnV3RsZQ--

Twin car bombs kill 28 near bank in Baghdad. Two suicide car bombers struck a crowded area outside a state-run bank June 20 in Baghdad, killing nearly 30 people in the latest attack targeting a high-profile part of the capital. The blast, which tore the glass facade off the three-story Trade Bank of Iraq building, leaving chairs and desks exposed, occurred shortly after 11 a.m. as the area was packed with people at the start of the local work week. Iraqi officials initially said the explosives-packed cars were parked a few hundred yards apart, but later said the attacks were staged by suicide bombers. The chairman of the Trade Bank of Iraq — which was established to facilitate international trade and reconstruction efforts after the 2003 U.S.-led invasion — said five guards were among the dead, and that six others were wounded. "The work of building Iraq's economic strength ... goes on uninterrupted, as does the work of the bank, which will be open for business tomorrow," the chairman said in a statement after the attack. Source: http://www.google.com/hostednews/ap/article/ALeqM5hwK_CSpBxsNuVUEaDuOwmSSCiqGwD9GF5QJ00

BANKING AND FINANCE INDUSTRY

Woman arrested on explosives charge ahead of G-20. The common-law wife of a man charged with possession of explosives in what police are calling a Group of 20 summit-related arrest has also been charged in the investigation. A police spokeswoman said June 24 that the 37-year-old suspect has been charged with possession of an explosive device and possession of a weapon. The suspect's partner, a computer-security expert, was charged June 23 with several offenses, including possession of explosives, dangerous weapons and intimidating a justice system participant. An Internet activist and contributor to the Canadian Broadcasting Corp. said the computer expert told a May meeting of activists and professors that he planned to monitor police chatter about the summit of the Group of

UNCLASSIFIED

UNCLASSIFIED

Twenty Finance Ministers and Central Bank Governors (G-20) summit and post it on Twitter. He also said he would buy items online to attract police attention. The police spokeswoman said she could not say what the explosives are but said there is no risk to public safety. Police have declined to release more details, but police said the investigation is part of the ongoing effort to ensure a safe and secure G-20 Summit in Toronto. The G-20 groups the leaders from 19 leading rich and developing nations, and the European Union. Source: http://www.insidebayarea.com/news/ci_15365963

Credit card data breaches cost big bucks. Javelin Strategy & Research estimates that credit and debit card issuers spent \$252.7 million in 2009 replacing more than 70 million cards compromised by data breaches. In 2009, an estimated 39 million debit cards and 33.3 million credit cards were reissued due to data breaches, for a total of 72.2 million. An estimated 20 percent of those affected by the breaches had more than one card replaced. Javelin's survey shows that 26 percent, or one out of four U.S. consumers received a data-breach notification last year from a company or agency holding their personal data, including credit and debit card or checking account information. Of the people notified (which is required by law in most states), 11.5 percent were victims of identity fraud compared with only 2.4 percent who were not notified. The report surmises that data breaches lead to fraud. Digital Transactions explains, "Data breaches are one obvious pathway to fraud, but a breach alone doesn't mean an affected consumer will become an identity-fraud victim. Banks often give free credit-report monitoring services to customers whose data may have been compromised." The flaw here is that credit monitoring only makes the consumer aware of new account fraud, when a Social Security number is used to open a new account. Credit monitoring has nothing to do with credit card fraud in which an existing account is compromised. "There's a disconnect," Javelin tells Digital Transactions News. Consumers "should pay attention to your credit reports after you're notified, because you're more vulnerable." Source:

http://advice.cio.com/robertsiciliano/10816/credit_card_data_breaches_cost_big_bucks

(Colorado; New Mexico) FBI investigates credit card scam. More than 270 credit card accounts were used in purchases across the country after the computer systems at two Serious Texas Bar-B-Q restaurants in Durango, Colorado were breached between February and April, a FBI special agent said. The FBI took over the case after people in the region filed reports with law enforcement agencies. The security breach was mitigated in late April, and the company no longer is vulnerable to the cyber thieves, he said. If people paid for a meal at either restaurant with a credit or debit card during the breach, their account numbers still may be in the hands of crooks. The chief operating officer at Citizen's Bank in Farmington, New Mexico said some of the bank's customer account numbers were stolen, though he would not say how many. The consumers will get their money back after they go through a "dispute process," he said. The co-owner of Serious Texas Bar-B-Q said the problem was a nationwide attack against companies who used Aloha Software. He said his company was notified of the security breach by Mastercard in April, and the restaurant spent \$600 to have its software upgraded by April 28. Two weeks ago, the restaurant was contacted by Durango police, which said people who ate at the restaurant during the three-month security breach were reporting fraudulent charges. Source: http://www.daily-times.com/ci_15331917

Security budgets stable or increasing at financial firms. Despite the current global recession, information-security budgets at financial institutions generally are staying stable, and many even have increased, according to a study conducted by accounting and consulting firm Deloitte. The seventh annual survey of security spending and priorities at financial institutions worldwide, released

UNCLASSIFIED

UNCLASSIFIED

June 17 found that 56 percent of information-security budgets have increased. Additionally, the survey found there was a 20 percent drop this year in the percentage of respondents who said a lack of sufficient budget is a major barrier to information security (36 percent in 2010, compared to 56 percent in 2009). Further, respondents at more than 70 percent of organizations said they are planning to implement at least one new security technology in the next 12 months. When it comes to security priorities, the largest percentage of respondents cited identity and access management followed by data protection, security-infrastructure improvement, regulatory and legislative compliance and compliance remediation. Source: <http://www.scmagazineus.com/security-budgets-stable-or-increasing-at-financial-firms/article/172793/>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nuclear dumps argue over diluting waste for burial. A competition between nuclear waste dumps has pulled the Nuclear Regulatory Commission (NRC) into an unusual reconsideration of its rules to allow moderately radioactive materials to be diluted into a milder category that is easier to bury. At issue is whether a site in Utah that is licensed to accept only the mildest category of radioactive waste, called Class A, could accept far more potent materials, known as Class B and C wastes, by blending the three together. Even low-level, radioactive waste is a growing problem, with few licensed repositories to dispose of it. The problem dates from the early 1980s. Around the country, the inventory of low-level wastes with no place to go is growing by about 10,000 cubic feet per year. EnergySolutions of Salt Lake City has asked state regulators in Tennessee for permission to blend wastes together there so they would qualify for disposal in its dump in Clive, Utah, in the desert about 80 miles west of Salt Lake. If allowed, it would open a potentially vast market to the company. A rival company, Waste Control Specialists of Andrews, Texas, is arguing that a repository it hopes to open late this year, specifically for B- and C-class wastes, would provide better protection in case an intruder blundered onto the site in the future. The company also says it could provide less expensive service to waste producers like hospitals if it had a bigger market. The NRC heard arguments June 17 from representatives of each company, as well as radiation-safety officials from three states, the lawyer for a company that processes waste for burial, and an expert from a group that opposes nuclear power. Source: <http://www.nytimes.com/2010/06/18/business/energy-environment/18nuke.html>

COMMERCIAL FACILITIES

Man arrested near G20 security site. A 53-year-old Toronto man is under arrest after a G-20 Summit bike patrol found a cache of weapons, including a crossbow, in a car that was pulled over June 24. The car was stopped near the secure zone of the Group of Twenty Finance Ministers and Central Bank Governors summit in Ontario, Canada. Officers found three arrows, containers of gas, a slingshot, chainsaw, fire axe, saws, a tire iron, and other items in the vehicle. The accused also had a large piece of plywood that police suspect was for use in scaling G-20 security fences, officers said. The suspect, whose identity wasn't released by police, was driving an older model Hyundai Elantra that looked suspicious, police said. The suspect was stopped near the Novotel Hotel, where employees are on strike. Late June 24, police wearing rubber gloves were searching the vehicle, which had Ontario plates. The old car, which had a hand-made roof rack, was cordoned off with police tape. Officers weren't sure if they were going to call a bomb squad to examine the vehicle. Police from a hazardous-material unit were called to examine a second area that was roped off because of a possible gasoline

UNCLASSIFIED

UNCLASSIFIED

spill. The suspect is expected to appear for a bail hearing June 25. The investigation is continuing. Source: <http://www.torontosun.com/news/g20/2010/06/24/14501761.html>

(Missouri) Cape man arrested for making bomb threats. Cape Girardeau, Missouri police June 24 arrested a local man who they say made bomb threats against West Park Mall in Cape Girardeau, and the Walmart in Jackson, Missouri. A lieutenant of the Jackson Police Department said the store was cleared just after 4 p.m. While they didn't think there was any real danger, he said police took precautions. Walmart management made the decision to evacuate the store, he added, and police assisted. By 4:30 p.m., business was back to normal at the Jackson store. A spokesman for the Cape Girardeau Police Department said no bomb was found at the mall. Source: <http://www.semissourian.com/story/1645143.html>

Shots fired near G20 security zone. Police are searching for a black BMW that fled from the Toronto, Canada entertainment district early June 22 after shots were fired near the G20 security zone. At least three shots were fired from a vehicle near John St. and King St. W around 3:15 a.m. investigators said, despite an increased police presence in the area. While the shots were fired close to the yellow G20 security zone, where more than 5,000 police officers are set to patrol downtown Toronto, police said they have no reason to believe this incident is related to the upcoming summit. Investigators said three shell casings from a small caliber gun were found in the area, but could not confirm reports that police vehicles pursued the vehicle to the city's west end where it disappeared, or that more than a dozen off-duty Royal Canadian Mounted Police officers witnessed the shooting. Nobody was injured and the investigation is ongoing. Source: <http://www.thestar.com/news/gta/article/826739--shots-fired-near-g20-security-zone>

COMMUNICATIONS SECTOR

(Oregon) Amateur radio operators aid government communications during emergencies. Amateur radio operators, who use various types of radio communications equipment for nonprofit purposes, can provide a valuable resource to state and local governments during disasters. In Oregon, about 1,800 Radio Amateur Civil Emergency Service (RACES) volunteers are authorized to work in state and county emergency operations centers (EOCs) facilitating communication during disasters. For example, during the Great Coastal Gale of 2007 that knocked out communications to Columbia, Clatsop and Tillamook counties, ham radio operators used a radio-frequency messaging system called Winlink to transmit requests for assistance to the state's Office of Emergency Management (OEM). Following the storm, Oregon's governor funded improvements to the state's amateur radio infrastructure with a \$250,000 grant for Winlink systems in each of the state's 36 county-level EOCs. Amateur radio operators can play a variety of roles that allow public safety officials to maximize their resources, including facilitating communications; providing emergency managers with on-scene situational awareness; and helping manage large-scale events, such as state fairs and marathons. Earlier this year as blizzards blanketed Delaware, RACES members manned ham radio stations at the Sussex County EOC, and others drove around the county's 958 square miles reporting what they were seeing and confirming reports from the National Weather Service. Source: <http://www.govtech.com/gt/articles/765536>

(California) After fiber-optic sabotage, AT&T builds backup. More than a year after sabotaged fiber-optic cables in South San Jose, California left the county without phone and Internet service, working

UNCLASSIFIED

UNCLASSIFIED

credit card machines or cash-spitting ATMs, AT&T is building a backup “information highway” over the Santa Cruz Mountains to help prevent a similar outage. The new lines will not be used to enhance local AT&T Internet, television or phone service, he said. Currently, AT&T’s main information cables to Santa Cruz County run from San Jose to Salinas, around the Santa Cruz Mountains and back up the coast, he said. So when a chainsaw-equipped vandal opened a manhole early April 9, 2009, and sliced key fiber-optic lines, he left much of three counties without wireless technology and land-line telephone service until that evening. While the cut cables belonged to AT&T, many were leased to Verizon. As a result, both providers were out of commission. Meanwhile banks closed, coffee shop baristas scribbled credit card numbers to run later and newspaper readers cleaned out racks around town, unable to access the World Wide Web. Law enforcement patrolled cities and the county in force because residents could not call in emergencies. Source:

http://www.santacruzsentinel.com/localnews/ci_15348017

(Oregon) The secret of the ooze: Who did this? And why. Feynman Group employees are still wondering what suspicious substance was spread around their building on the morning of June 22, which closed the Eugene, Oregon computer-consulting and Web-hosting business for two hours. Investigators and Haz-Mat crews from the Eugene Police Department (EPD) and the Eugene Fire Department collected samples of the noxious yellow liquid and turned them over to Oregon State Police. An EPD spokeswoman did not know when results would be available. One employee was sent to the hospital after being exposed to the substance. A witness noticed the liquid spilling onto the sidewalk from a newspaper delivery box propped near the Feynman Group entrance as he arrived for work. He spotted more yellow liquid spread near the front door and near the door to a computer storage room on the side of the building. Not knowing what he was dealing with, he smelled the liquid and poured the newspaper delivery box out into the parking lot. The liquid smelled like ammonia, then sulfur when it was poured out, he said. It started smoking once poured out. Other than a bad cough that developed after he inhaled the fumes, the man is doing fine. Whatever the substance was, Eugene Police believe it was spread on purpose. Source:

<http://www.kval.com/news/local/96938549.html>

(Pennsylvania) Verizon warns of scammers ‘phishing’ for account information. The manager of media relations at Verizon Communications Inc. said Erie, Pennsylvania residents should be on the lookout for suspicious people posing as Verizon employees. Lately, there have been e-mails going around that ask for updated information. This scam is known as phishing. These e-mails will generally tell customers that their account will be interrupted if they do not update their account information. The claims are not true, and account information should not be provided. Source:

<http://www.goerie.com/apps/pbcs.dll/article?AID=/20100621/NEWS02/306219925/-1/news>

AT&T, Verizon join Wi-Fi roaming group. AT&T and Verizon Wireless, the two largest U.S. mobile operators, have joined an organization that ensures roaming among mobile operators’ Wi-Fi networks. The group, called the Wireless Broadband Alliance (WBA), also announced June 21 that South Korean mobile operator KT, Cisco Systems, U.S. cable operator Comcast, and wireless software vendor Devicescape Software have recently joined. The WBA provides for sharing of log-in credentials among operators of Wi-Fi networks so that subscribers can log into another WBA member’s network using the same username and password as they do with their primary carrier. Service providers that join WBA commit to participating in this program over time, though the interoperability may not be available immediately, said the CEO of Devicescape. AT&T and Verizon were not immediately able to

UNCLASSIFIED

UNCLASSIFIED

confirm what they will be doing with the WBA. Also June 22, the WBA said it is set to release the WISPr 2.0 specification, which will allow Wi-Fi network operators to go beyond the single-log-in capability and remove the need for entering any username and password for roaming. Source: [http://www.computerworld.com/s/article/9178362/AT T Verizon join Wi Fi roaming group](http://www.computerworld.com/s/article/9178362/AT_T_Verizon_join_Wi-Fi_roaming_group)

FCC meets with broadband providers over regulation. Phone and cable company representatives have been meeting with the Federal Communications Commission (FCC) to discuss giving the government authority over high-speed Internet lines. The FCC is seeking comment from broadband providers, including AT&T and Verizon Communications, and Internet companies, such as Google and Skype, to see if they can find common ground over the FCC's power to regulate broadband Internet companies. Talks were held June 21 with the chief of staff for the FCC chairman. A similar meeting was held June 18, a day after the FCC voted to gather public comments on whether the agency should reclassify broadband regulation under existing stricter, older phone-network regulations. Phone and cable companies have urged Congress to update the Communications Act so that the FCC doesn't resort to using the decades-old rules for broadband lines. Source: <http://www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=225700991&subSection=All+Stories>

Ipswitch survey reveals corporate bandwidth use across Europe to double during World Cup. Ipswitch Inc.'s Network Management Division, developer of the WhatsUp Gold suite of innovative IT management solutions, today released the results from its World Cup Network Traffic Calculator. Over the past two weeks, WhatsUp Gold has collected over 1000 responses related to average bandwidth use and the predicted increase during the 30 days of the tournament in network traffic directly related to the World Cup. According to the calculator, bandwidth use is expected to increase by 38.85% in participating World Cup Nations to 86.89% during matches. In Europe the figure is expected to double, from 40.25% current average bandwidth use, to 78.67% during key match times. In the UK, despite the culture for some businesses to close during England matches, bandwidth use is still expected to increase by 30.79% to 71.85% of total capacity. In host nation South Africa, IT Managers are bracing themselves for network bandwidth to be completely maxed out to 100% from a base average of 58% during a typical working day. Despite not being typically thought of as a football watching nation, the US is somewhat surprisingly expecting bandwidth use to rise to over 80% during some key matches. Source: <http://www.sbwire.com/press-releases/sbwire-48201.htm>

FCC group crafting plans to open up mobile spectrum. The Federal Communications Commission (FCC) Spectrum Task Force laid out preliminary ideas June 18 for making frequencies now used for satellite services available for conventional mobile broadband. The group is considering proposing to the FCC a Notice of Proposed Rulemaking for the satellite-related radio spectrum that would be presented at the Commission's next meeting July 15. The task force was formed recently to execute an intention stated in the National Broadband Plan for freeing up 500MHz of spectrum for mobile broadband by 2020. The group will propose that frequencies be allocated within the "S" band — one of three bands in the mobile satellite services range — for pure terrestrial wireless broadband services, either fixed or mobile, said the group's co-chair, who also heads the FCC's Office of Engineering and Technology. Currently, holders of spectrum in that band can only build terrestrial networks to complement their satellite systems. The FCC has already taken action to make more spectrum available for mobile broadband. Earlier this year, it approved the acquisition of satellite phone service provider SkyTerra, which holds spectrum in the "L" band, by Harbinger Capital

UNCLASSIFIED

UNCLASSIFIED

Partners. By 2015, Harbinger plans to deploy a terrestrial 4G (fourth-generation) mobile data service that can be used in conjunction with its satellite offering, according to the FCC. This could create another high-speed mobile network that would compete with those of the major carriers, while including some service to rural areas that many cellular networks don't reach today. Source: http://www.computerworld.com/s/article/9178238/FCC_group_crafting_plans_to_open_up_mobile_spectrum

DEFENSE INDUSTRIAL BASE SECTOR

Targeted Trident cyber-attack against defense company. Targeted attacks occur when cybercriminals launch malware against a specific organization, industry or government department. In recent years, such attacks have been distributed in the form of booby-trapped Word documents or malformed Adobe PDF files. Overnight, Sophos intercepted an attack against a firm working in the defense industry. The e-mails carried a malicious PDF file claiming to be about the Trident D-5 missile, launched from nuclear submarines. The malicious hackers behind the attack forged the "from:" address, pretending that the e-mail was a communication from an employee of Lockheed Martin. In this case they used the real name, e-mail address and phone number of one of Lockheed Martin's PR team - details which can be found easily on the Web - to make the message appear more plausible. The ZIP attachment contained a file called "TRIDENT D-5 MISSILE.PDF," which itself contains embedded JavaScript and SWF code to exploit vulnerabilities and deliver a malicious payload to the recipient's computer. The purpose appears to be to open a backdoor on the infected computer through which the hacker will be able to remotely access sensitive information. Source: <http://www.sophos.com/blogs/gc/g/2010/06/24/targeted-trident-cyberattack-defence-company/>

Northrop Grumman's APG-81 radar sensor performs flawlessly on first mission systems flight of Lockheed Martin F-35 aircraft. Northrop Grumman Corporation's new APG-81 active electronically scanned array (AESA) radar met and exceeded its performance objectives successfully tracking long-range targets as part of the first mission systems test flights of Lockheed Martin's F-35 Lightning II BF-4 aircraft. "During the F-35 flight, the Northrop Grumman APG-81 radar met and exceeded performance expectations, tracking long-range targets at all aspect angles with excellent stability. We look forward to working with Lockheed Martin in demonstrating the APG-81's high-resolution synthetic aperture radar (SAR) and other advanced capabilities on subsequent test flights," said the vice president of combat avionics at Northrop Grumman's Electronic Systems sector. Source: [http://nosint.blogspot.com/2010/06/northrop-grummans-apg-81-radar-sensor.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+\(Naval+Open+Source+INTelligence\)](http://nosint.blogspot.com/2010/06/northrop-grummans-apg-81-radar-sensor.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence))

CRITICAL MANUFACTURING

(Washington) Hoquiam police investigate Westport shipyard theft. Hoquiam, Washington police are investigating a burglary that took place at the Westport Shipyard June 17. Unknown suspects apparently entered the property by using a bolt type cutter to cut a hole in the chain link fence that surrounds the business nearest Ingram Street. Once inside the fence, the suspects cut the padlocks off and entered seven large, Conex-type shipping containers used for storage. An initial report estimated that approximately 800 pounds of rubber-coated copper wire was removed from several containers. About 500 pounds of the wire was described as 10-gauge, black-coated copper wire. Also

UNCLASSIFIED

UNCLASSIFIED

taken from some of the other containers were a brass relief valve, some stainless steel deck plates (two inscribed with the word “oil” and four with “diesel”). There were also a number of brass couplers and six items that are classified as brass nipples. All these items are used in the building of boats. The suspects apparently cut a larger hole in another section of the fence and used a wheelbarrow, which they found on the property, to wheel the stolen items to a grassy area behind the facility. Source: <http://kbkw.com/modules/news/article.php?storyid=1686>

EMERGENCY SERVICES

(Wisconsin; Minnesota) Official: Sirens aren’t saviors when storms hit. Parts of La Crosse, Wisconsin could have the same lack of sirens to warn of oncoming severe weather as reported in two Midwestern communities hit by tornadoes in the past week. Two of La Crosse’s nine tornado sirens — both early 1960s models — are not in working order, city officials said. It sets up a similar situation to Rochester, Minnesota, and Waukesha County in southeastern Wisconsin, where sirens failed to sound as severe storms swept in. A West Avenue siren is permanently disabled, and workers are troubleshooting problems with one on Diagonal Road on the city’s south side, said the assistant public works director who oversees city sirens. While having new sirens would be ideal, the system is not intended to be the primary means of warning people in an emergency, officials said. “People have to realize that these sirens are available, but are not your best source,” said the administrator of emergency services for La Crosse County. “We need to have people tune into the media to keep informed.” Source: http://lacrossetribune.com/news/state-and-regional/wi/article_76a51b34-7e80-11df-b6be-001cc4c03286.html

(Arizona) Police chief: Cartels threaten U.S. law enforcement in Arizona. In the first public incident of its kind, drug cartels are making direct death threats to U.S. law enforcement officials in Nogales, Arizona, the police chief there told CNN Monday. Speculation about death threats by cartels towards U.S. law enforcement has been widespread for some time, but this is the first time border officials confirmed a case. The threats began less than two weeks ago, after off-duty police officers from the Nogales police department seized several hundred pounds of marijuana from a drug-smuggling operation they stumbled upon while horseback riding, the chief said. The smugglers managed to flee into Mexico before they could be detained. “We are taking the threats very seriously,” the police chief said. “We have received information from informants who work in Mexico that the drug cartel running that operation was unhappy about our seizure. They told our informant that they understand uniformed police officers have a job to do, but anyone out of uniform who gets involved will be targeted. America is based on freedom. We’re not going to be intimidated by the threats, but we are taking them seriously. I’ve told my officers if they venture into that area off duty to be armed,” the police chief said. Source:

<http://edition.cnn.com/2010/CRIME/06/21/cartels.threats/index.html?hpt=T2>

ENERGY

US PHMSA promises extra scrutiny of BP onshore oil, gas pipelines. The U.S. Pipeline and Hazardous Materials Safety Administration (PHMSA) has given extra scrutiny to BP’s network of onshore oil and gas pipelines in light of the Deepwater Horizon disaster, the department’s head told a Senate panel Thursday. The PHMSA Administrator told the Senate Committee on Commerce, Science and Transportation that she recently met with the president of BP Pipelines and “explained to him that

UNCLASSIFIED

UNCLASSIFIED

we would be looking very closely at their program and doing an integrated inspection of their entire system.” The chairman of the National Transportation Safety Board said the Liberty project and the Endicott pipeline deserve attention. “We would want to make sure that they have adequate remote control shutoff valves, that they have corrosion protection, that the pipeline is marked,” she said. A Texas Senator asked whether two deadly natural pipeline blasts this month in her state demonstrate the need for more efforts to prevent excavation accidents, in particular. The PHMSA Administrator said both accidents were “absolutely preventable” and that more work needs to be done on public awareness, pipeline markings and other safety measures. Source:

<http://www.platts.com/RSSFeedDetailedNews.aspx?xmlpath=RSSFeed/HeadlineNews/Oil/6140414.xml>

Smart grid security to become multibillion-dollar industry. With the U.S. electrical grid — and other national grids worldwide — poised to become smart systems with integrated communications, the possible threat of sabotage has become an obvious concern. To that end, the U.S. government has set aside funding to develop security protocols. Others are following suit. Between 2010 and 2015, the report predicts, about 15 percent of all smart-grid investments will be spent on cybersecurity. This will represent a total global investment of \$21 billion over the next five years, according to the report. North America will spend the most with a predicted annual figure of \$1.5 billion by 2015, followed by Asia Pacific at \$1.2 billion and Europe at \$784 million. Evidence collected in 2009 found that the U.S. electrical grid is vulnerable to sabotage, and that it had been compromised by hacker spies testing the smart grid system’s access. Since then, there has been a major push by government and industry experts to better secure smart grids. Source: http://news.cnet.com/8301-11128_3-20008552-54.html

A surge protector to end all surge protectors. If an equipment failure, terrorist attack, or lightning strike causes a power surge, also known as a fault current, that current can cascade through the grid and knock out every substation and piece of equipment connected to the problem site. The Department of Homeland Security (DHS) Resilient Electric Grid project aims to develop a superconductor cable designed to suppress fault currents that can potentially cause permanent equipment damage. Communications of the ACM reports that the DHS Science and Technology Directorate is supporting a technological advance that could reduce the chances of similar blackouts occurring in the future. The Directorate’s Homeland Security Advanced Research Projects Agency (HSARPA) helped fund the development of an electrical cable that could be used to link substations, providing backup sources of electricity in the event part of the grid experiences an outage. The Resilient Electric Grid project will help ensure the nation’s utilities can withstand power surges that cause blackouts. Part of the project is the development of a superconductor cable designed to suppress fault currents. This technology will allow electric companies to link substations without running the risk of fault currents cascading through the electric grid. Source:

<http://homelandsecuritynewswire.com/surge-protector-end-all-surge-protectors>

FOOD AND AGRICULTURE

Brazilian beef products recalled for drug residues. Sampco, Inc. of Chicago, Illinois is recalling approximately 61,000 pounds of cooked canned and frozen beef products that may contain the animal drug Ivermectin, the U.S. Department of Agriculture’s (USDA’s) Food Safety and Inspection

UNCLASSIFIED

UNCLASSIFIED

Service (FSIS) announced June 24. Ivermectin is an antiparasitic used to de-worm live animals. In May, FSIS discovered residues of Ivermectin above the U.S. Food and Drug Administration's (FDA's) tolerance level for beef muscle in products from Brazil, which sparked an 87,000 pound Class II recall, with low-health risk, for related beef products, also from Sampco. The agency believes the recently recalled product may have entered the country through a separate route of entry. The following products are subject to recall: 12 oz. cans of "Deltina Corned Beef With Juices" with the production code "100120" on the top of the can. These products were sent to a distribution center in Florida for retail sales; 12 oz. cans of "Hormel Corned Beef With Natural Juices" with the production code "100120" on the top of the can. These products were sent to distribution centers in Guam for retail sales; 35 lb. boxes of frozen "Seasoned Cooked Beef." These products were distributed to federal establishments for processing; and 35 lb. boxes of "Sampco Brand Frozen Cooked Beef, Salt Added." These products were distributed to federal establishments for processing. Each product package bears "BRASIL 337 S.I.F," as well as "Product of Brazil" or "Packed under Brazilian Government Inspection." The products subject to recall were produced in Brazil on January 20, 2010. Source: <http://www.foodsafetynews.com/2010/06/brazilian-beef-products-recalled-for-drug-residues/>

(California) USDA orders recall of 143 million pounds of beef. A slaughterhouse that has been accused of mistreating cows agreed Sunday to recall 143 million pounds of beef in what federal officials called the largest beef recall in U.S...

www.cnn.com/2008/HEALTH/02/17/beef.recall/index.html

(California) South Gate Meat Co. recalls ground beef products due to possible E. coli contamination. South Gate Meat Co. of South Gate, California is recalling approximately 35,000 pounds of ground-beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced June 23. The products subject to recall include boxes labeled "South Gate Meat Co." of varying sizes, including: 20-, 30- and 40-pound bulk packages marked "Ground Beef"; 30-, 40-, and 50-pound bulk packages marked "Coarse Ground Beef"; and 10- and 20-pound packages marked "Ground Beef Patties." Each package bears establishment number "EST. 6217" inside the USDA mark of inspection. These products were produced between the dates of June 7, 2010, through June 21, 2010, and were shipped to restaurants in the Los Angeles and Orange County, California, area. Source: http://www.imperialvalleynews.com/index.php?option=com_content&task=view&id=7505&Itemid=1

(Connecticut; New Jersey; New York) New York company issues ground beef recall over E.coli concerns. A Long Island food company has recalled approximately 3,700 pounds of ground beef that may be contaminated with E.coli, the U.S. Department of Agriculture (USDA) said June 22. The products subject to recall include boxes labeled "W.B. Stockyard, Keep Refrigerated" in a variety of sizes, including: 24, 8-ounce burgers in 12-pound boxes marked "Burger Fresh, WB Home Style"; 32, 6-ounce burgers in 12-pound boxes marked "Burger Fresh"; 48, 4-ounce burgers in 12-pound boxes marked "Burger Fresh"; 10-pound boxes marked "Beef Ground/Extra Lean"; and 10- and 20-boxes marked "Beef Ground 80/20". According to the USDA recall, each package bears establishment number "EST. 20889" inside the USDA mark of inspection as well the Julian dates of "10164" and "10166." These ground beef products were produced June 11, 2010, and June 15, 2010, and were shipped to food-service institutions in Connecticut, New Jersey and New York. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.nbcnewyork.com/news/local-beat/New-York-Company-Issues-Ground-Beef-Recall-96917119.html>

USDA announces quarantine to prevent spread of citrus disease. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is issuing an interim rule announcing a plant quarantine in several states and territories to stop the spread of citrus greening, a plant disease that greatly reduces citrus production, destroys the economic value of the fruit, and can kill trees. The interim rule replaces all previous federal orders related to citrus greening, expands areas under quarantine, allows additional treatment options and provides exemptions for certain fully processed products, such as curry leaves and kaffir leaves. The interim rule is placing under quarantine the states of Florida and Georgia, the territories of Puerto Rico and the U.S. Virgin Islands, two parishes in Louisiana, and two counties in South Carolina due to the presence of citrus greening. Interstate movement of certain plant material and products (except fruit and certain processed products) will be restricted or prohibited from quarantine areas. Citrus greening is considered to be one of the most serious citrus diseases in the world. Once the host plant becomes infected, there is no cure for the disease. In areas of the world where the disease exists naturally, citrus trees decline and die within a few years and may never produce usable fruit. Source:

http://www.freshplaza.com/news_detail.asp?id=65063

Soybean rust confirmed in Southern U.S. Soybean rust has been reported on soybeans in the southern United States for the first time this year. "The first find of soybean rust was reported in Texas on June 10, on the border with Mexico. Current predictions for other southern states is that they won't begin to detect it for another 4 weeks at the earliest because of unfavorable weather conditions for the disease to spread," said an Ohio State University Extension plant pathologist with the Ohio Agricultural Research and Development Center. Since its discovery in the United States in 2004, researchers have learned quite a bit about soybean rust, including that the disease is manageable. Kudzu is an overwintering host for the disease, but not all kudzu species are susceptible. The amount of inoculum is greatly reduced over winter. Several effective fungicides have been identified. Soybean rust is UV light sensitive. Sunlight can actually kill spores. The development and spread of the disease is highly weather dependent. The disease does not appear to jump onto soybeans from other hosts until after flowering during the prime growing season; this does not hold true for soybeans that emerge during the winter in the southern U.S. Source:

<http://www.wisconsinagconnection.com/story-national.php?id=1225&yr=2010>

ARS and New Mexico Scientists take a long look at livestock and locoweed. Keeping livestock away from poisonous locoweed during seasons when it's a forage favorite is one way ranchers can protect their animals and their profits, according to a 20-year collaboration by Agricultural Research Service (ARS) scientists, and their university partners. The ARS researchers teamed up with New Mexico State University (NMSU) scientists to study locoweed poisoning in U.S. livestock. When livestock graze on locoweed, the plant's toxic alkaloids can sicken and sometimes kill the animals, which can cost U.S. producers millions of dollars every year. The research involved identifying fungal species that produce locoweed toxins, assessing toxin-level variations, finding biomarkers that could help pinpoint toxicity levels in animals that had consumed locoweed, assessing the effect of locoweed toxins on animal reproduction and livestock-grazing preferences, and evaluating herbicide and biological control of the weed. Results from the research were published in the journal *Rangelands*. Source:

<http://www.ars.usda.gov/is/pr/2010/100621.htm>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Texas) Burnet County Courthouse briefly evacuated due to suspicious activity. On June 24, the Burnet County Courthouse in Burnet, Texas was evacuated for about two hours in response to a suspicious activity investigation. About 9:50 a.m., the Burnet County Sheriff's Office was notified that an unidentified male was observed leaving two unattended suitcases in the vicinity of a bench located on the first floor of the courthouse. Upon locating the suitcases and consulting with the Austin Police Department Bomb Unit, the courthouse and surrounding buildings were evacuated until the arrival of the bomb unit. As the investigation progressed, the identity of the owner of the suitcases was determined. The man was questioned and released after the bomb unit determined that the contents of the suitcases were not hazardous. The courthouse and surrounding buildings were reopened at approximately 11:45 am. No charges are expected to be filed in this incident. Source: http://www.statesman.com/blogs/content/shared-gen/blogs/austin/blotter/entries/2010/06/24/burnet_county_courthouse_brief.html

(Kentucky) Lewis County Courthouse evacuated after bomb threat. The Lewis County Courthouse in Vanceburg, Kentucky was evacuated June 24 after officials said a bomb threat was received. The Lewis County deputy said the call was received about 10:15 a.m. The caller said there were three bombs in the Vanceburg area but only mentioned the location of one, which he said was in the courthouse. The deputy clerk received the call then called the sheriff's office. A search was conducted by members of the sheriff's department and the Kentucky State Police. The call was cancelled soon after. The deputy said he believes the call was a hoax, but the sheriff's department intends to find the perpetrators. The deputy said the caller could be charged with wanton endangerment or terroristic threatening, possibly up to 75 counts, one count for each person who was in the courthouse at the time the threat was received. Source: http://www.maysville-online.com/news/local/article_90054d06-800b-11df-b084-001cc4c002e0.html

AWOL Afghans found ... on Facebook. At least 11 of the 17 members of the Afghan military who went AWOL from an Air Force base in Texas have turned up on Facebook. Some belong to the "Afghanistan Mujahideen" group, a page that features, among other content, videos from the American-born al Qaeda spokesman Azzam the American. According to a nationwide be-on-the-lookout (BOLO) bulletin that was sent by the North Texas Joint Terrorism Task force to law enforcement agencies across the country the week of June 14, the 17 Afghan deserters walked away from the Defense Language Institute at Lackland Air Force Base, where they had been studying English. The men have military identification that would give them access to secure U.S. military installations, the bulletin read. One week later, an Immigration and Customs Enforcement source said that only two or three of the 17 Afghans remain at large. The source said investigators have been working with Canadian immigration records and now believe that many of the men are in Canada. A spokesman for Randolph Air Force Base in Texas said he was told that four of the men remain unaccounted for. Of the 13 who have been located, he said, six have pending refugee claims in Canada, two have permanent residency in Canada, four are in the process of being deported, and one is a conditional resident alien in the U.S. Source: <http://www.foxnews.com/us/2010/06/25/exclusive-awol-afghans-found-on-facebook/>

UNCLASSIFIED

(Arizona) Mesa street lamps get protection from thefts. After losing more than \$1 million to copper thieves, Mesa, Arizona is boosting the security of street lights. Mesa's transportation department is installing alarm systems on the electrical junction boxes wired to street lights. "Thieves have stripped us of more than 34 miles of copper wire this year," Mesa's transportation department superintendent said. "It has cost the city over \$275,000 to replace and repair." Now when thieves break into the electrical junction boxes, a loud, piercing alarm will sound, alerting nearby residents to contact the police. Officers are also working with scrap metal recycling sites to catch copper thieves. Copper is worth about \$2 per pound. Mesa's transportation department claims thieves can steal hundreds of pounds of copper wire from just one electrical junction box. The city of Mesa has 27,000 electrical junction boxes, according to the transportation department. They plan to install the alarm systems at boxes in known trouble areas. The boxes will also have a warning label on top, informing would-be thieves that tampering with city property is a felony. Source:

http://www.abc15.com/dpp/news/region_southeast_valley/mesa/mesa-street-lamps-get-protection-from-thefts-

(Oregon) National Guard alerts members that personal information is at risk. The Oregon National Guard took on a new mission Tuesday, identifying and notifying soldiers whose personal information may be at risk after a laptop was stolen from a Guard member's vehicle in the Portland area. "It could potentially affect a lot [of people]," said a spokesman for the Oregon National Guard. "I don't have enough information to say just how many." The theft was reported Monday to the Portland Police Bureau. The National Guard released information about the security breach late Tuesday. "Although this laptop is password-protected, with potential exposure of individual personal information, we are doing everything possible to notify individuals about the theft," the spokesman said. The laptop, which the Guard member was using to conduct work from home, may have contained the sensitive personal information of service members, including Social Security numbers, the spokesman said. The Oregon National Guard and the National Guard Bureau are contacting people whose personal information may have been compromised. Source:

<http://www.statesmanjournal.com/article/20100623/NEWS/6230424/1001#ixzz0rgdOVDUj>

Chinese breaking into classified network. The Chinese may have been able to develop computer algorithms that will penetrate military computers at the secret level, according to alerts about a "Spear Phishing attack" issued recently to users of a military system, said a report in Joseph Farah's G2 Bulletin. In one case, users of military computers at the secret, or collateral, level told of a false report of an outbreak of war in Asia beaming across military networks. "So, it appears they're into our systems at least at the collateral level," one military computer user said of the Chinese. He said such access is "relatively hard to get into." In earlier cases, Trojans and viruses also have been introduced that halted the use of flash drives on Defense Department computers. While it remains unclear whether the Chinese have developed algorithms that would allow penetration systems that are Top Secret or beyond, it cannot be ruled out, since the Chinese have developed super computers capable of developing encryption and decrypting codes. Most U.S. troops in the field use classified information at the collateral level. Collateral information includes reporting on combat arms and tactical operations. If that is the case, then the enemy could be given access to codes capable of decrypting collateral traffic and could, in effect, be reading intelligence that may be going to U.S. war fighters in Afghanistan and Iraq. Source:

<http://www.wnd.com/index.php?fa=PAGE.view&pageId=169365>

UNCLASSIFIED

UNCLASSIFIED

(Colorado) Suspect sought over bomb threat: Suspicious item found to be non-explosive. At 1:01 p.m., Saturday, the Sterling, Colorado Emergency Communication Center received a 911 call from the payphone at the 7-11 store located at 311 W. Main St. The caller advised there was an explosive device on Front Street in Sterling. The Sterling Police Department responded to the area and conducted a search for suspicious items. During the search, an officer located a suspicious device in a city trash receptacle located in front of the Logan County Chamber of Commerce office in the 100 block. The surrounding area was evacuated and area streets were closed. Due to the circumstances, the Greeley Bomb Squad was notified and responded to the scene. After further investigation, the suspicious device was determined not to be an explosive. At approximately 6:30 p.m., the area was re-opened. A description of a person of interest was obtained by officers. This person was seen in the immediate area of the payphone at the time the call was made, and is described as a white male in his mid- to late-40s, about 6'2" tall with a slender build. The man was possibly wearing a tan baseball-style hat and tan shirt. Source:

<http://www.istockanalyst.com/article/viewiStockNews/articleid/4236329>

Lots of security incidents at military bases, but no connection seen. The lockdown Monday morning of a Naval Air Engineering Station in Lakehurst, New Jersey, is the latest in a number of security incidents at the gates of U.S. military bases across the country. While the incidents have been close together, the FBI, local police and the U.S. Army's Criminal Investigative Command (CID), have found no connection and no link to terrorism. Monday's incident involved a delivery truck driver who told a guard at the gate at Lakehurst that he had a legal firearm. That happened just as there were false reports of gunshots near another gate of the same base. The base was locked down for an hour and after an investigation, the driver was allowed to leave. The incident followed by days a shooting at Fort Gillem, Georgia, in which a soldier was shot and killed, allegedly by a fellow soldier. Prior to that two men were arrested at MacDill Air Force Base in Florida, on suspicion of trying to bring unauthorized weapons onto the base that houses the headquarters of the U.S. Central Command. Source: <http://edition.cnn.com/2010/US/06/21/military.base.security/?hpt=T2>

(Texas) Man threatens to throw grenade into downtown government building. A man in San Antonio, Texas is accused of calling the U.S. Department of Agriculture (USDA) more than 20 times and threatening to use a grenade to kill employees. Police said the suspect was upset about his taxes and he made the calls to complain. That is when he got violent and threatened to throw a grenade through a window in the USDA's building on Durango Boulevard Downtown. The suspect is now facing a charge of a making a terroristic threat against the government. Source: http://www.woai.com/news/local/story/Man-threatens-to-throw-grenade-into-downtown/PAowNu_q4Ue9095DsH_ILQ.csp

(Texas) Capitol evacuated after Friday bomb threat. Four weeks to the day after metal detectors came in use at the Texas State Capitol in Austin, a bomb threat forced the Department of Public Safety (DPS) to evacuate the capitol and another government building. It happened around 11 a.m. Friday. According to DPS, somebody called 9-1-1 and made a threat. The capitol, along with a district DPS office at 15th and Congress, were evacuated, while officers searched the both buildings for explosives. Nothing was found. The DPS office opened first. The capitol reopened around 2 p.m. DPS has now opened a criminal investigation into the threat. Source: <http://www.kens5.com/news/Capitol-evacuated-after-Friday-bomb-threat-96686459.html>

UNCLASSIFIED

UNCLASSIFIED

(Indiana) Phishing attacks on Ball State accounts continue. A phishing attack on Ball State University e-mail accounts could still be a threat to its users. University Computing Services (UCS) has worked in clearing damaged computers, but faculty and students at the Muncie, Indiana institution were still receiving bogus e-mails June 18. A few employees' accounts were compromised since the e-mail's detection June 15, the senior systems security communications manager said. However, UCS is working to clear infected accounts and filter out any phishing spam sent to the university and urges students, faculty and staff to not reply to any unsolicited requests of confidential information. Phishing is the term used to describe an attempt to obtain passwords or other personal information from e-mail users, often by getting them to click on a link that installs "malware," or malicious software. The bogus e-mail sent to Ball State users claims to be from the school's "Webmail Administrator" and urges the user to click on a link. Source: <http://www.bsudailynews.com/phishing-attacks-on-ball-state-accounts-continue-1.2275894>

FBI found 14 intel leak suspects in past 5 years. The Federal Bureau of Investigation identified 14 suspected "leakers" of classified U.S. intelligence information during the past five years, according to newly disclosed statistics. Between 2005 and 2009, U.S. intelligence agencies submitted 183 "referrals" to the Department of Justice (DOJ) reporting unauthorized disclosures of classified intelligence. Based on those referrals or on its own initiative, the FBI opened 26 leak investigations, and the investigations led to the identification of 14 suspects. "While DOJ and the FBI receive numerous media leak referrals each year, the FBI opens only a limited number of investigations based on these referrals," the FBI explained in a written response to a question from a Democratic Senator from Rhode Island. "In most cases, the information included in the referral is not adequate to initiate an investigation. The most typical information gap is a failure to identify all those with authorized access to the information, which is the necessary starting point for any leak investigation. When this information is sufficient to open an investigation, the FBI has been able to identify suspects in approximately 50 percent of these cases over the past 5 years. Even when a suspect is identified, though, prosecution is extremely rare (none of the 14 suspects identified in the past 5 years has been prosecuted)," the FBI said. Source: http://www.fas.org/blog/secretcy/2010/06/intel_leak.html

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Kraken botnet making a resurgence, researcher says. The Kraken botnet — one of the Internet's largest and most difficult to detect in 2008 — is rearing its ugly head again. In fact, the old security nemesis — which was reported dismantled last year — has compromised more than 318,000 systems, nearly half of the 650,000-node size it achieved at its peak in 2008, according to a research scientist at the Georgia Tech Information Security Center (GTISC), a leading authority on botnet research. So far, the resurrected Kraken is primarily a spam distributor, focusing most of its output on ads for male enhancement and erectile dysfunction. The botnet's performance is prodigious: a single node with a DSL-speed connection was detected sending more than 600,000 spam messages in a 24-hour period. Many popular antivirus tools do not detect Kraken. A scan by VirusTotal indicates that none of the top three antivirus tools — Symantec, McAfee, and Trend Micro — can detect current Kraken samples, he reports. The resurrected Kraken is usually installed by another botnet, using botnet malware such as Butterfly, the researcher reports. It is not clear whether Kraken installation is handled by the same criminal group as Kraken operations, but it may be an example of specialized criminal groups working together, he suggests. Kraken's reappearance may indicate a broader trend toward the re-use of code. Source:

UNCLASSIFIED

UNCLASSIFIED

http://www.darkreading.com/vulnerability_management/security/antivirus/showArticle.jhtml?articleID=225701438&subSection=Antivirus

Inside text message phishing attacks. Not all phishing takes place online. Text-message-based phishing, called smishing, is still out there, and though on the decline, a report from security vendor Internet Identity (IID) shows it is still being used to target credit unions. In smishing, scammers use text messages to impersonate companies and lure victims into calling a fake interactive voice response (IVR) system designed to steal personal data like account credentials and Social Security numbers. “The most common text phishing is text-to-phone, where text messages are sent to potential victims with the goal of getting those victims to call a phone number provided in the message,” explained the CEO of IID. “When a victim calls the number, they are presented with an interactive voice response tree that often mimics the target institution’s own system. This system draws out and collects account access credentials from the victims.” Less common is text-to-Website, where the text message lures the victim to a traditional phishing Website, he added. According to the CEO, the attack patterns suggest there are no more than a few groups perpetrating text-phishing attacks as opposed to several dozen perpetrating other forms of phishing. IID reported the prevalence of the attack dropped 62 percent during the first quarter of 2010. Source:

http://securitywatch.eweek.com/phishing_and_fraud/inside_text_message_phishing_attacks.html

Twitter accounts hacked. More than 1,000 Twitter accounts have been compromised by hackers, according to F-Secure researchers. The hacked accounts are subsequently used to tweet “Hacked By Turkish Hackers.” The researchers are currently unclear how the hacking attack is spreading. However, it appears that significant numbers of compromised accounts are owned by Israelis. One researcher suggests, “Perhaps there’s a Twitter phishing run in Hebrew underway?” Twitter has seen a variety of phishing attacks, as cyber criminals look to exploit the latest trends in user behavior. Source: <http://www.thenewnewinternet.com/2010/06/23/twitter-accounts-hacked/>

Report says be aware of what your Android app does. About 20 percent of the 48,000 apps in the Android marketplace allow a third-party application access to sensitive or private information, according to a report released June 22. And some of the apps were found to have the ability to do things like make calls and send text messages without requiring interaction from the mobile user. For instance, 5 percent of the apps can place calls to any number and 2 percent can allow an app to send unknown SMS messages to premium numbers that incur expensive charges, security firm SMOBILE Systems concluded in its Android market-threat report. SMOBILE said that while not all apps are malicious, there is the potential for abuse. Users should know what the apps they downloaded are doing because they have expressly granted the apps permission to do those activities when they downloaded them. In addition, the Android architecture limits the apps to the permissions granted so any damage from a potentially malicious app would be very limited, according to Google. The report found that dozens of apps have the same type of access to sensitive information as known spyware does, including access to the content of e-mails and text messages, phone-call information, and device location, said the chief technology officer at SMOBILE Systems. Source:

http://news.cnet.com/8301-27080_3-20008518-245.html?part=rss&subj=news&tag=2547-1_3-0-20

The truth about social media identity theft. The use of social media can increase consumer vulnerability to identity theft because of the amount and type of personal information people share on these networks. However, consumers do little or nothing to protect themselves, according to a

UNCLASSIFIED

UNCLASSIFIED

recent study by the Ponemon Institute. Although more than 80 percent of study respondents expressed concern about their security while using social media, more than half of these same individuals admitted they do not take any steps to actively protect themselves. This data clearly demonstrates that while people may acknowledge that security is important, many do nothing to protect their information online. Other key findings from the survey include the following: approximately 65 percent of users do not set high privacy or security settings in their social media sites; more than 90 percent of users do not review a given Web site's privacy policy before engaging in use; approximately 40 percent of all respondents share their physical home address through social media applications; and surprisingly, people who have been victims of identity theft are just as likely to be lax in securing their personal information online. Study results from identity-theft victims and non-victims are virtually identical. Source: <http://www.net-security.org/secworld.php?id=9445>

Most firms face security 'red alert' as XP SP2's retirement looms. Three out of four companies will soon face more security risks because they continue to run the soon-to-be-retired Windows XP Service Pack 2 (SP2), said a report published June 22. Toronto-based technology systems and services provider Softchoice Corp. said that 77 percent of the organizations it surveyed are running Windows XP SP2 on 10 percent or more of their PCs. Nearly 46 percent of the 280,000 business computers Softchoice analyzed rely on the aged operating system. "This is a red alert," said Softchoice's services development manager. "This isn't something you can safely ignore." He was referring to the impending end-of-support deadline that Microsoft Corp. has set for Windows XP SP2, a service pack that debuted in the fall of 2004. After July 13, Microsoft will stop issuing security updates for SP2, a move that has users scrambling to update to Windows XP SP3, which will be supported until April 2014. "Windows XP SP2 is deployed in 100 [percent] of the companies [surveyed] to some extent," said the manager. "But that doesn't tell the whole story. On average, 36 [percent] of the PCs in every organization run SP2." Softchoice obtained its data from customers of its IT assessment services, which include asset, hardware life cycle and licensing management. It analyzed PCs in 117 U.S. and Canadian organizations in education and the financial, health care and manufacturing industries. The firm weighted the number of XP SP2 systems in each polled organization to arrive at the average usage mark of 36 percent. Source: http://www.computerworld.com/s/article/9178378/Most_firms_face_security_red_alert_as_XP_SP2_s_retirement_looms

Malware: certified trustworthy. According to anti-virus vendor F-Secure, the number of digitally signed malware samples for Windows is increasing - and more and more scareware programs also include a valid digital signature. Virus authors use this method to overcome various hurdles on Windows systems, and suppress alerts such as those triggered when a program attempts to install an ActiveX control in Internet Explorer, or before installing a driver. F-Secure's list of potentially undesirable programs contains almost 400,000 digitally signed samples. In terms of malware, the list still includes almost 24,000 samples. Authenticode is used for signing and checking software under Windows and is meant to verify the origin of software. Users tend to trust digitally signed software. Software without a digital signature triggers a dialogue that explicitly asks the user for confirmation before proceeding with the installation. In the 64-bit versions of Windows 7 and Vista, installing an unsigned driver isn't possible at all, even if a user were to wave it through. F-Secure said that virus authors successfully use various tricks to obtain valid digital signatures or certificates for their programs. The most reliable method is to trick a Certificate Authority into issuing a code-signing certificate. It seems that this has become just as easy as obtaining a valid SSL server certificate - a

UNCLASSIFIED

UNCLASSIFIED

valid e-mail address is sufficient. Internet frauds and criminals also use such services as Digital River, which sign software for their customers. Source: <http://www.h-online.com/security/news/item/Malware-certified-trustworthy-1027066.html>

Automatic web encryption (almost) everywhere. The HTTPS Everywhere extension for Firefox automatically redirects users to secure SSL connections when they access certain Web pages – if this is supported by the server. Jointly developed by the Tor Project and the Electronic Frontier Foundation (EFF), the extension was inspired by the search engine modification Google implemented to make browsers send all their search queries via HTTPS. Google had previously already adjusted its Google Mail service so that Web-browser connections to the service are protected via SSL by default. This prevents attackers from accessing sensitive data (even in unsecured wireless networks). HTTPS Everywhere further expands this function and simply redirects the browser to the secure page by rewriting the URL. According to the developers, however, the extension first checks whether the page returns identical content via http and via https. At present, the plug-in is still in beta phase and only rewrites selected URLs, for instance those of Google Search, Wikipedia, Twitter, Facebook, The New York Times, The Washington Post, PayPal, EFF, Tor and Ixquick. However, it is relatively easy for users to add further rules for other domains. Source: <http://www.h-online.com/security/news/item/Automatic-web-encryption-almost-everywhere-1025472.html>

Apple sneaks anti-malware update into Snow Leopard. Ten months after it debuted rudimentary malware scanning in Snow Leopard, Apple this week quietly added a signature for a third piece of malware, security researchers reported June 18. According to U.K.-based antivirus vendor Sophos and U.S. Mac security company Intego, Mac OS X 10.6.4, which Apple released June 15, includes an update to XProtect. Dubbed that because the malware signatures are contained within Snow Leopard's "XProtect.plist" file, the feature debuted in August 2009 with the launch of Mac OS X 10.6. At the time, Apple included detection for only two pieces of malware, Trojan horses named "RSPlug.a" and "Iservice" by Symantec. The 10.6.4 update added a scanning signature for another Trojan, which Symantec has labeled as "HellRTS." According to Sophos, which calls the same Trojan "OSX/Pinhead-B," and like Symantec has had protection in place since April, hackers have disguised the threat as iPhoto, the photo-management software that ships with new Macs. The masquerade is meant to dupe users into installing the backdoor malware. Source: http://www.computerworld.com/s/article/9178227/Apple_sneaks_anti_malware_update_into_Snow_Leopard

Security firms taking days to block malware. Anti-malware vendors can take up to 92.48 hours to block malicious sites, potentially leaving clients in blissful ignorance of threats to their systems in the meantime. Security researchers ISS Labs reviewed a range of endpoint security products from 10 big-name security vendors and their response to "socially engineered or consensual malware threats." It said 15,000 to 50,000 such threats per day were presenting themselves. Effectiveness rates varied from a 35-percent block rate to 88.3 percent. Vendors' average times to respond to new threats ranged from 4.62 hours to 92.48 hours, with the high end turned in by Panda, IDC said. Of the 10 vendors profiled, just three managed response times of less than 30 hours. The researchers concluded that vendors with "in the cloud reputation systems" kept much more malware off their clients' desktops. However, most vendors do not have such systems, or, the report concluded, they are still immature and have yet to have an impact on detection rates. Vendors covered by the survey

UNCLASSIFIED

UNCLASSIFIED

were: AVG, Norman, ESET, Panda, F-Secure, Sophos, Kaspersky, Symantec, McAfee and Trend Micro. Source: http://www.theregister.co.uk/2010/06/21/malware_delays/

Zeus malware distributed via terror-themed spam. Spammers are notorious for latching on to the most recent trend in an effort to increase click rates. Recently, a spam campaign containing Zeus malware utilized recent concerns over terrorism to send messages which appeared to be sent by the Department of Homeland Security, Transportation Security Administration and Department of Defense. Researchers at Sophos Labs have discovered a low-yield campaign that targets government users with enticing subjects like “Report on Defending and Operating in a Contested Cyber Domain” and “RE: Al-Qaeda in the Arabian Peninsula.” “Unlike some of the other Zbot runs we’ve seen, this current run is relatively low volume,” writes a SophosLabs Canada researcher in a blog post. “Nevertheless, this trickery by the Zbot crew is not new. They’ve tried to spoof other agencies such as the NSA (National Security Agency) back in February, going as far as coming up with a spam run that ‘reports’ on their own attacks.” The e-mails contain links to the supposed reports, which actually are zip files containing the Zeus Trojan. Source: <http://www.thenewnewinternet.com/2010/06/21/zeus-malware-distributed-via-terror-themed-spam/>

NATIONAL MONUMENTS AND ICONS

Studies confirm pollution in national parks. From 2003 to 2005, scientists from the United States, the United Kingdom, and New Zealand studied pollution issues in eight U.S. national parks and preserves. Pollution was found in all eight sites including, Rocky Mountain, Glacier, Olympic, Sequoia, and Mt. Rainier National Parks in the Pacific Northwest. Scientists said most of the pollution was caused by regional agriculture or industry, including pesticides, the burning of fossil fuels, industrial operations and other sources. Of the areas studied, the largest problems with pesticides were found in Sequoia, Rocky Mountain and Glacier National Park. An associate professor at Oregon State University said pesticides appear to be the biggest concern, which can accumulate in the ecosystem and food web. Scientists said the research should provide a better understanding of the risks, including which pesticides are most likely to accumulate and may require improved regulation. Source: <http://kezi.com/news/local/178826>

(Colorado) Strong winds stoke spread of Medano fire. Infrared map data from a late-night flight June 19 showed that the Medano Fire in Huerfano and Saguache counties continued to burn predominately on the Great Sand Dunes National Park and Preserve in Colorado, with the fire growing to 4,541 acres. Moderate rates of spread were observed by firefighters during periods of strong afternoon winds June 20. The eastern flank of the fire has burned onto the San Isabel National Forest San Carlos Ranger District. Hot, dry, and windy weather is expected to continue through the middle of the week, creating conditions favorable for sustained fire growth. Lightning June 6 ignited the fire approximately 4 miles north of the park’s visitor center near Little Medano Creek. The fire information officer for the Type-2 Incident Management Team said the aerial flights were not started until June 18 — and then again on June 19 — because it had been too windy to get the planes up. Flights are made at night or in the early morning when it is cooler. Fire managers began implementing containment strategies along the eastern flank of the fire June 20. There is still no indication when the fire will be considered under control. Source: http://www.chieftain.com/article_d466725a-7cef-11df-bfb7-001cc4c002e0.html

UNCLASSIFIED

UNCLASSIFIED

(Pennsylvania) **Aryan Nations rally remains peaceful despite threats.** On June 19, Aryan Nations members and protesters shouted threats to spill blood and other acts of violence across the lawn at Gettysburg National Military Park in Pennsylvania. The Aryan Nations identifies itself as a white-supremacist organization, and the group has been named a “continuing terrorist threat” by the FBI. Although park officials said they do not support the views of the group, they are still obligated to accommodate those exercising their First Amendment rights. Multiple law enforcement agencies were in attendance during the two-hour rally, including local and national park police as well as officers from Cumberland Township and Gettysburg borough. K-9 units patrolled the surrounding areas and a National Park Service helicopter buzzed overhead. The white supremacists carried no visible weapons, despite earlier statements from a Aryan Nations leader saying the group would be armed. Instead, members brandished flags representing the Aryan Nations, the Confederacy, and white supremacy. Both Aryan Nations members and protesters were required to pass through police checkpoints — where backpacks and pockets were searched for potential weapons — before allowed access to the rally. Protesters were held in check by police forces. Separating the roughly 70 protesters from Aryan Nations members was about 60 yards of open lawn. Police barricades kept the groups apart and officers were posted around the area. Source: http://www.ydr.com/ci_15333463

(Arizona) **Up in smoke: Schultz fire chars 5,000 acres; 750 homes evacuated.** Three hundred firefighters are battling a 5,000-acre wild-lands fire burning northeast of Schultz Pass in Arizona. No structures had been lost as of June 20, but containment was at 0 percent. The Schultz fire was reported around 11 a.m. June 20 near Forest Road 420 — Schultz Pass Road. It was the second major wildfire in two days. The Hardy fire south of I-40 Saturday burned 300 acres and forced 170 homes to be evacuated. Officials on Sunday evacuated Horse Camp along FR 556 and about 750 homes in nearby Timberline and Wupatki Trails neighborhoods west of Highway 89. About 170 animals from the Second Chance shelter were moved to the Fort Tuthill County Park. The shelter had previously been an evacuation site for animals at the Coconino Humane Association, which was evacuated June 19 in response to the Hardy fire. Northbound Highway 89 was closed at Silver Saddle Road. Southbound Highway 89 was closed 2 1/2 miles north of Sunset Crater. The Sunset Crater and Wupatki national monuments were closed and evacuated. Source: http://www.azdailysun.com/news/local/article_b533ea2a-f302-5748-b8b9-e7d966dffde4.html

POSTAL AND SHIPPING

(Illinois) **White powder closes Scott AFB building.** A building at Scott Air Force Base in Belleville, Illinois was briefly closed June 24 in response to a possible hazardous material scare. A secretary in building 1961, which houses part of U.S. Transportation Command, was opening mail when she found a white, powdery substance in one of the envelopes around 9 a.m., according to information provided by Scott Air Force Base. The letter was addressed to a senior leader who works in the building. Parts of the building were evacuated and the area was cordoned off. Hazardous-material and bioenvironmental technicians as well as fire and medical teams responded to the report of the substance. The powder was tested and found negative for biological or chemical material. The area was declared safe around 11 a.m. The substance will undergo additional testing, and the Office of Special Investigations will continue to investigate the incident. Source: <http://www.military.com/news/article/white-powder-closes-scott-afb-building.html?ESRC=topstories.RSS>

UNCLASSIFIED

UNCLASSIFIED

(Texas) Dallas city hall offices briefly quarantined after white substance found. The mayoral suites on the fifth floor of Dallas City Hall in Dallas, Texas were briefly quarantined June 23 when an assistant to the mayor pro tem opened a package and a suspicious white substance fell out. Police and fire hazardous materials crews quickly determined the substance was not harmful but did not immediately confirm what it was. The mayor pro tem said he was informed by officers that the substance was cocaine and that it was believed to have been sent by someone known to police. The deputy chief said police would open a criminal investigation into the matter. He said that the substance couldn't immediately be identified and that it hadn't been field-tested as a drug. The mayor pro tem said the person who sent the substance had attempted to harass him before. He suggested that the letter sender has mental problems. Source:

http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-caraway_24met.ART.East.Edition1.2946c44.html

(Florida) Gateway Blvd reopens after suspicious package report. Lee County, Florida deputies have reopened Gateway Boulevard, which was shut down because of a suspicious package. Gateway was closed between Towne Lake Drive and Commerce Lakes Drive for over two hours. The road reopened just before 3 p.m. The suspicious package was delivered to the local FBI office on Commerce Lakes Drive. The office was evacuated around 12:45 p.m. The Southwest Florida Regional Bomb Squad responded and detonated the package. Source: <http://www.nbc-2.com/Global/story.asp?S=12683632>

PUBLIC HEALTH

New disaster toolkit assists special needs populations. A new toolkit “meant to assist state and local public health agencies improve their emergency-preparedness activities” for special-needs populations has been released under a project funded by the Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response. Executed by the Center for Public Health Preparedness within RAND Health, the toolkit “distills the most relevant strategies, practices, and resources from a variety of sources.” The report of the program that developed the toolkit, Enhancing Public Health Emergency Preparedness for Special Needs Populations: A Toolkit for State and Local Planning and Response, stated that “experiences from recent emergencies, such as Hurricanes Katrina and Rita, have shown that current emergency preparedness plans are inadequate to address the unique issues of special needs populations.” Source:

<http://www.hstoday.us/content/view/13706/149/>

(Florida) Bomb threat called in to doctor's office. A building in North Miami Beach, Florida was evacuated June 22 after someone called in a bomb threat to a doctor's office. North Miami Beach police said someone called a doctor's office and said, “There is a bomb in the building.” Police evacuated the building. Investigators searched the doctor's office and nearby businesses and found nothing dangerous. Source: <http://www.justnews.com/news/23990199/detail.html>

The optimal balance of vaccine stockpiles. Once a disease has been eradicated, there is a danger it could reappear, either naturally or as a result of an intentional release by a terrorist group; how much vaccine should be produced and stored for a disease that may never appear again — or which may infect hundreds of thousands tomorrow? Stockpiling vaccines for eradicated diseases poses particular difficulties. A model that could be used to guide public health decisions about how much vaccine to

UNCLASSIFIED

UNCLASSIFIED

stockpile against an eradicated disease, such as smallpox, is published in the June 11 edition of Vaccine. A researcher and colleagues from Delft University of Technology in the Netherlands are the first to use mathematical tools to give the best balance of the various factors that enable optimal emergency stores of a vaccine to be held after a disease has been wiped out. They devised their model using research studies and reports that detail these factors, which include delays in producing large quantities of reagents used in the vaccines, and the time needed to fill the individual vaccine vials needed for immunization campaigns. The time needed for safety and efficacy testing, and constraints in vaccine distribution and administration are additional considerations. The model takes these issues into account to arrive at the “optimal balance” between the financial costs of the vaccine, production speed, and the public health costs of leaving people unvaccinated. Source: <http://homelandsecuritynewswire.com/optimal-balance-vaccine-stockpiles>

EarlySense gets FDA nod for improved patient monitoring system. Israeli medical device company EarlySense Ltd. has received Food and Drug Administration (FDA) clearance to sell its EverOn Touch patient-monitoring system in the United States. Based in Ramat Gan, Israel, the company also is pursuing European market clearance for the enhanced system. EverOn is a patient-supervision system that goes underneath a hospital bed mattress. The device measures patients’ vital signs, such as heart and respiration rates, as well as movements to alert caregivers about their medical condition. “We have repeatedly heard from our partner hospitals that preventing pressure ulcers is a critical need due to the enormous burden pressure ulcers place on hospital budgets and the huge task of preventing them,” EarlySense’s chief executive said in the release. Source: <http://www.medcitynews.com/2010/06/earlysense-gets-fda-nod-for-improved-patient-monitoring-system/>

TRANSPORTATION

TSA lags on risks to intermodal transport. The Transportation Security Administration (TSA) has not conducted full risk assessments across all major aviation and surface transportation modes; therefore, it lacks a comprehensive picture of the terrorist threats to those systems, congressional investigators said in a report Monday. The National Infrastructure Protection Plan (NIPP) prescribes a six-step, risk-management process that TSA started to follow in 2007 with a National Transportation Sector Risk Analysis. It abandoned that effort, however, and later intermittently assessed threat, vulnerability, and consequence in the transportation modes of aviation, mass transit and passenger rail, freight rail, highways, and pipelines, according to the Government Accountability Office (GAO). “However, a risk assessment, as required by the NIPP, involves assessing each of the three elements of risk and then combining them together into a single analysis,” stated the GAO report, Transportation Security: Additional Actions Could Strengthen the Security of Intermodal Transportation Facilities. In 2007, TSA started its National Transportation Sector Risk Analysis, which would have estimated threat, vulnerability, and consequence for a set of terrorist-attack scenarios and then would have integrated those estimates to score each scenario and compare the scores across the various modes of transportation. But TSA later abandoned the project “due to difficulties in estimating the likelihood of terrorist threats,” the GAO report stated. Specifically, the Department of Homeland Security (DHS) and TSA could do more for its personnel by providing workforce planning and training of employees; more for its management processes by coordinating activities with key stakeholders in transportation security; and more for technology by improving testing for

UNCLASSIFIED

UNCLASSIFIED

technologies for supporting security programs, the study said. Source:

<http://www.hstoday.us/content/view/13690/128/>

FAA asks American to re-inspect 767's. The Federal Aviation Administration has advised American Airlines to re-inspect 56 of its Boeing 767 jets after cracks were detected on at least two planes. A Fort Worth-based American spokesman said the carrier detected the problem and “we caught them when they should have been caught. The cracks were discovered on a part that attaches the engines to the wings.” The spokesman said 54 planes had been inspected by Monday, and American has sent one of the cracked pylons to an outside company for metallurgy testing. The inspections have not caused any major disruption to American’s schedule. Source:

http://www.seattlepi.com/local/6420ap_tx_american_jet_inspections.html

Congress authorizes passenger guns in Amtrak luggage. An obscure provision tucked into a transportation funding bill last year has now been interpreted as a permanent right for passengers to carry guns aboard Amtrak, the federally funded passenger train service. The Government Accountability Office earlier this month informed a senator of Mississippi that language he inserted into the 2010 transportation appropriation bill will be ongoing and not expire September 30. The language allows Amtrak passengers to have guns in their checked baggage, something not allowed since the September 11 terrorist attacks. An Amtrak spokesman said June 15 the railroad has just submitted to Congress its plan for implementing the language including tightening security, changing its reservation system so that passengers can notify Amtrak when they intend to travel with a gun, adding new signage for area where guns are stored, and implementing education programs for the public and law-enforcement agencies. Source:

<http://www.capitolnewsconnection.org/?q=node/14868>

(Illinois) Chicago subway fire sends 19 to hospital. A fire in a Chicago subway injured 19 people and sent black smoke billowing from grates along city streets. The Chicago Transit Authority said heavy smoke was reported around 5 p.m. June 20 along the Red Line tracks just north of downtown. The fire was quickly extinguished and investigators are trying to determine what started the blaze. Nineteen people were taken to hospitals, most with respiratory complaints, though none suffered life-threatening injuries. Five people were transported in serious to critical condition, three were in fair to serious condition, and 11 had minor injuries. Source:

<http://www.businessweek.com/ap/financialnews/D9GFLB00.htm>

(Florida) TSA workers find loaded gun in man’s luggage. A man was arrested June 19 for having a loaded handgun at the Orlando International Airport. The handgun was found in the man’s carry-on luggage. The Transportation Security Administration said the pistol was loaded when they caught it at a security checkpoint. The man was released on bond. Why he had the weapon in his luggage remains unknown. Source: <http://www.wesh.com/news/23969171/detail.html>

(California) LAX terminal evacuated on false report of explosives. A man who falsely claimed to be carrying an explosive at Los Angeles International Airport June 19 prompted the closure of the Tom Bradley Terminal before police shot him with a stun gun and took him into custody. The incident began when the suspect grabbed a passenger’s luggage outside of the terminal, ran inside and claimed the package contained a bomb. The terminal was evacuated for 20 minutes as officers

UNCLASSIFIED

UNCLASSIFIED

pursued the man inside the facility. The package he was carrying did not contain explosives. Source: <http://latimesblogs.latimes.com/lanow/2010/06/lax-tom-bradley-terminal-evacuated-.html>

WATER AND DAMS

Billions spent to protect world water: study. Billions of dollars — mainly from China — are being poured into a fast-growing global system of rewards for people who protect endangered water resources, according to a study released Wednesday. The programs, implemented by governments as well as the private sector and community groups, “could help avert a looming global water quality crisis,” according to the report by Ecosystem Marketplace, a project of US-based non-profit organization Forest Trends. It said the “emerging marketplace” of watershed payments and trading in pollution-reduction credits was still dwarfed by the system of carbon trading aimed at limiting damaging greenhouse gases, but was expected to rise. The study focused on two main instruments, Payments for Watershed Services (PWS), in which farmers and forest communities are compensated for maintaining water quality, and Water Quality Trading (WQT) where the industry buys and sells pollution-reduction “credits”. Transactions support a range of activities including adjusting land-management practices, technical assistance, and improving water quality, according to the report funded by the United States and the Netherlands. The report conservatively estimated the total transaction value of active PWS and WQT initiatives at \$9.3 billion worldwide in 2008. This included about \$7.8 billion, all of it in PWS schemes, from China where the central government has called for development of “eco-compensation mechanisms”. Source:

<http://www.google.com/hostednews/afp/article/ALeqM5iwt2nVi9yduMMt7rdvIvRHCMTs6Q>

Asian carp found beyond Chicago area barrier. Federal and state officials in Illinois said June 23 that they found a live bighead or Asian carp in Lake Calumet in Chicago, 6 miles from Lake Michigan, in an area near where a poisoning operation that ended June 4 took place. The creature, found by commercial fishermen looking for carp as part of wider carp-hunting missions, was 34.6-inches long and weighed just under 20 pounds. Asian carp present a threat to native species because they can grow upwards of 100 pounds and quickly take over the ecosystem where they reside. This is the first time anyone has found an Asian carp, live or dead, beyond an electric barrier on the Chicago Sanitary and Ship Canal near Lockport. The nearest carp to the barrier was a dead one found last December after a massive poisoning of the shipping canal. The fish was probably about 3 to 4 years old, old enough to reproduce, officials said. Although found alive, it is now dead and will undergo testing to determine if the fish was born and bred in the wild, or raised in aquaculture for the food trade.

Source: <http://www.freep.com/article/20100623/NEWS06/100623047/1001/NEWS/Asian-carp-found-beyond-Lake-Michigan-barrier>

(Nebraska) Ten dams fail in central Nebraska. Continued rain has people across Nebraska watching creeks, rivers, and dams. Ten dams failed in central Nebraska amid the heavy rains and storm run-off that caused widespread flooding in the last week, the Nebraska Emergency Management Agency (NEMA) said Saturday. Several rivers swelled to near-record levels after last weekend’s deluge, and state assessment teams continue to survey damage to bridges, roads and other infrastructure. Residents in northeast Nebraska were bracing for more rain Saturday, and flooding was still being reported along some rivers. The failed dams were in Atkinson, Burwell, North Loup, Sargent, Scotia, Spalding and Taylor, NEMA officials said. Most caused little damage, but the failure of Bredthauer Dam added water to the swollen Mira Creek and may have contributed to the need to evacuate

UNCLASSIFIED

UNCLASSIFIED

North Loup last Saturday. A flood warning still is in effect for the Elkhorn and Platte rivers in Dodge County. Forecasters at the National Weather Service in Valley said the Platte River in North Bend should rise above the 8-foot flood stage this afternoon to reach 8.9 feet by Tuesday. It should be back under flood stage by early Thursday. The Elkhorn River near Hooper was expected to hit 17.5 feet the evening of June 21, 3.5 feet above flood stage. More rain also is in the forecast. Flooding also has closed several Nebraska highways. Source: http://fremonttribune.com/news/local/article_075361c6-7d47-11df-b9e4-001cc4c03286.html

(Texas) Drug cartel activity threatens Texas water supplies, lawmaker says. Drug cartel activity along the Mexican border presents serious security threats to the area's water supply system, particularly on federally-owned lands in southern Texas, a U.S. lawmaker said. Members of the House Natural Resources Subcommittee on Water and Power held a hearing June 17 on H.R. 4719, a bill that would create a Southwest Border Region Water Task Force to monitor and assess the water supply needs of the area. The California representative told FoxNews.com that the situation needs immediate attention, particularly in light of reports that a Mexican drug cartel — the Los Zetas — unsuccessfully plotted to blow up the Falcon Dam along the Rio Grande last month. "If the plot against Falcon Dam had succeeded, it would have affected more than 4 million residential customers," he said Monday. According to the Houston Chronicle, Mexican and U.S. authorities were "secretly scrambling" last month to thwart a plot by the Zeta cartel to blow up Falcon Dam and unleash billions of gallons of water. Sources told the Chronicle that U.S. officials learned of the plot through "serious and reliable sources," the seizure of small amounts of dynamite near the dam, and the discovery of an alert from the Zeta cartel warning Mexican residents to evacuate the area ahead of the blast. Source: <http://www.foxnews.com/politics/2010/06/21/drug-cartel-activity-threatens-texas-water-supplies-lawmaker-says/?test=latestnews>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7): 866-885-8295(IN ND ONLY);** Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED